ISSN 0956-9979 JANUARY 1999

# VIRUS BULLETIN

THE INTERNATIONAL PUBLICATION ON COMPUTER VIRUS PREVENTION, RECOGNITION AND REMOVAL



## *IN THIS ISSUE:*

• **And they're off!** This month's comparative review for DOS saw VB 100% awards given to eight out of the sixteen competing products. Check out the winners on p.10.

• **Scoop!** This issue is fairly bursting with news stories, not all of them good publicity. Read who's been doing what for the last month, starting on p.3.

• **Thoroughly modern?** *Cheyenne InocuLAN* is now *CA InoculateIT*. We review this major new update for *NT* server on p.17.

## CONTENTS

# EDITORIAL

## Remotely Likely?

Cast your mind back a few months to the guest editorial in the May 1998 *VB*. There, our Technical Editor, Jakub Kaminski, discussed the most desirable approach to resolving issues that may arise from the discovery of security holes or similar flaws in a software product or system.

Although he did not mention it at the time, his thoughts were influenced by what some felt was ill-considered talk about a very serious security hole in the VBScript of *Internet Explorer*, as shipped in the final beta of *Windows 98*. He opined – correctly, I think – that ideally a group of industry experts should analyse the matter, outside the public's gaze. Some form of consensus was likely to arise from this and the quality and weight of that analysis should convince a possibly skeptical developer that it should act.

*"... raises questions about its motives and professionalism"*

But what *does* this have to do with Remote Explorer, I hear you ask.

I could have written about the gullibility and manipulability of the general, and the non-specialist but IT-oriented, media and how *NAI* ('formerly known as McAfee Associates' remember) is a past master of such. I could have railed against the increased lowering of the standard of acceptability for 'headline news' – whatever happened to 'independent corroboration'? Perhaps reporting 'NAI announced... Other experts contacted have not yet seen the virus...' passes the test these days?

I could point out that if one 'news' web site runs a story these days, the others seem compelled to follow suit. This quickly escalates the 'story', reinforcing its significance to the traditional media. Thus, a slot on the New York early-evening news can be assured by early afternoon in Santa Clara.

But I'll address concern for user security. *NAI* had an 'exclusive' in having Remote Explorer turn up at a customer site. It was a complex beast, but not difficult to deal with simply as a virus. Thus, providing samples to other researchers soon after finding it would have allowed other products to have detection updates produced quickly. But why would *NAI* do that?

*NAI* is in business, after all, and giving samples to competitors does not seem like a move to enhance the differentiation of its product from others. That is the raw business-school graduate's naïve analysis and completely inappropriate in the anti-virus industry. *NAI* should have provided samples of Remote Explorer to the rest of the anti-virus industry much sooner than 22 December.

According to unofficial reports from *MCI*, *NAI* was aware of the 'problem' one week prior to that date. Even if you take the official *NAI* line that it became involved on 17 December, and *if* the virus was as potentially destructive and mobile as the early *NAI*-sourced 'news' suggested, *NAI* had a moral responsibility to the computing community, independent of its status as an *NAI* customer, to ensure that maximum detectability was available.

This requirement was not met by *NAI* analysing the virus completely then providing its own detection and cleanup routines. Assuming that everyone will run your software is an arrogance usually associated with a software developer based further north on the US west coast. Sites that take security seriously have policies preventing them using non-approved software. That a major vendor of network security solutions seems unaware of this in the face of driving up media hysteria around Remote Explorer raises questions about its motives and professionalism.

Eventually, *NAI* provided samples to the rest of the anti-virus industry. What did we find? Remote Explorer was not the world-killing virus John McAfee would have dreamed of. It was crude, buggy, obvious and should not be able to infect a well-designed and competently run NT network. Stifling scrutiny of Remote Explorer by others had one major 'benefit' for *NAI* – it prevented independent refutation of the claims made for it during the days running up to Christmas.

*NAI* might improve its reputation further by teaching senior executives what 'cyberterrorism' is and the manager of *McAfee Labs* to recognize cancer victim hoaxes before forwarding them to *VB*.

# NEWS

## Point of Infection

*PowerPoint* has fallen. The virus author responsible for several Visual Basic Script viruses (including the so-called 'HTML viruses' discussed in last month's *Virus Bulletin*) released PP97M/Vic.A (also known as Attach), the first *PowerPoint* macro virus in early December 1998.

Anti-virus researchers are at odds as to the likely success of *PowerPoint* viruses relative to *Word* and *Excel* viruses. Initially, many thought *Excel* macro viruses were very unlikely to become widespread as it was felt XLS files were not widely shared. Without good statistics on how commonly PPT files are shared, current estimates are little more than guesses based on an individual's experience of file-sharing patterns. Despite this however, Attach seems unlikely to be much of a threat, as (rather arbitrarily), it only infects PPT files which include forms.

Just before this issue went to press Attach's author released PP97M/Shaper.A (also known as ShapeShift) and a day later PP97M/Master.A (ShapeMaster). These do not require the host to include forms and are thus more likely to spread. Fortunately, the default options in *PowerPoint* warn users when they open files containing macros and the viruses do not disable this.

The arrival of *PowerPoint 97* viruses adds another complex file format to the list for which anti-virus developers have to write parsers. *PowerPoint 97* slide shows are OLE2 files, so existing OLE2 parsing code should be easily adapted to deal with them. Further parsimony should be found in that the internal format of the *PowerPoint's* VBA modules is very similar to that of its *Office 97* stablemates *Word* and *Excel*. There is, however, a twist – unlike in DOC and XLS formats, VBA modules (and most other components) are stored in a compressed form in PPT files.

Adding support for decompressing these components may slow the appearance of reliable detection of *PowerPoint* viruses in many anti-virus products ▮

## Class Act!

The week or so prior to Christmas is one of the news media's most notorious 'silly seasons'. Stories that might normally not even bubble high enough to be considered become major items and 'cat stuck in tree' stories can take the front page.

Thus, on 21 December 1998, *The New York Times* ran a story about a terrible new *Word* macro virus. 'Computer security experts' the story started 'are warning clients about a new software virus that is spread by e-mail, infects Microsoft Word files and has already caused several networks to crash.'

### Prevalence Table – November 1998

| Virus | Type | Incidents | Reports |
|---|---|---|---|
| Cap | Macro | 56 | 13.2% |
| Class | Macro | 34 | 8.0% |
| ColdApe | Macro | 30 | 7.1% |
| CIH | File | 29 | 6.8% |
| Hark | Macro | 28 | 6.6% |
| Temple | Macro | 27 | 6.4% |
| Parity_Boot | Boot | 25 | 5.9% |
| Laroux | Macro | 24 | 5.7% |
| Npad | Macro | 15 | 3.5% |
| AntiEXE | Boot | 10 | 2.4% |
| Concept | Macro | 10 | 2.4% |
| Groov | Macro | 9 | 2.1% |
| Brenda | Macro | 8 | 1.9% |
| Jumper | Boot | 8 | 1.9% |
| Munch | Macro | 7 | 1.7% |
| AntiCMOS | Boot | 6 | 1.4% |
| NYB | Boot | 6 | 1.4% |
| Win95/Marburg | File | 6 | 1.4% |
| DelCMOS | Boot | 5 | 1.2% |
| Quaint | Boot | 5 | 1.2% |
| ShowOff | Macro | 5 | 1.2% |
| Blee | Macro | 4 | 0.9% |
| Eco | Boot | 4 | 0.9% |
| Kenya | Boot | 4 | 0.9% |
| Nono | Macro | 4 | 0.9% |
| Wazzu | Macro | 4 | 0.9% |
| Appder | Macro | 3 | 0.7% |
| Baphometh.1536 | Multi-partite | 3 | 0.7% |
| Chack | Macro | 3 | 0.7% |
| Empire.Monkey | Boot | 3 | 0.7% |
| Form | Boot | 3 | 0.7% |
| Ripper | Boot | 3 | 0.7% |
| Russian_Flag | Boot | 3 | 0.7% |
| Others [1] | | 30 | 7.1% |
| **Total** | | **424** | **100%** |

[1] The Prevalence Table includes two reports each of: Angelina, Dodgy, Jerusalem.1363 and Tequila; and one report of each of: Beryllium, Bleah.D, Delwin, DeTroie, Ebola.6001, HLLC.Dosinfo, Imposter, Inexist, Int40, Junkie, LBB_Stealth, Manzon, NOP, Nottice, Paix, Quandary, Quicky.1376, Sampo, Stat, TPVO.3783, Unashamed and V-Sign.

Readers are reminded that more detailed listings are posted at http://www.virusbtn.com/Prevalence/.

A macro virus causing networks to crash sounded impressive, so *Virus Bulletin* read on… It turned out that this terrible 'new' scourge was the W97M/Class family, or perhaps more specifically the .B and .D variants of it, as suggested in the partial descriptions of its payloads.

This relatively inoccuous virus family has been known to virus researchers for some time; since mid June 1998 in the case of .B and early August 1998 for the .D variant. Its claim to fame was being the first 'class infector' – class viruses store their code in the ThisDocument stream (the name may vary in non-English versions of *Word*), rather than in a separate macro modules. [*The author of the first W97M/Class virus released an equivalent form of infector for* Excel 97*, X97M/Sugar, mid-December 1998. Ed.*]

There was, however, a significant effect following the release of Class. Many anti-virus products required their *Word* file-handling routines be modified to be able to check these VBA resources. In some cases, reliable implementation of these changes has only recently been available from some major vendors and many users had not updated their software. This allowed the variants that made it into distribution to establish healthy footholds in some regions.

How healthy? George Smith, editor of the Crypt Newsletter (http://www.soci.niu.edu/~crypt/), reported two weeks prior to the New York Times article that Class.D was running rampant at the US House of Representatives. Smith cheekily dubbed it 'an uninvited guest… for [the] impeachment hearings' in reporting that it was not initially detected by any of the various antivirus packages used at the House.

It is interesting that so much attention was focussed on such relatively harmless – even 'amusing' – viruses, particularly in North America. The obviousness of the payload, triggering on the 14th of months from June to December inclusive, seems a likely explanation for this. It is a pity that less obtrusive but much more damaging viruses do not grab the attention they deserve for lack of compliance with the Hollywood model virus, which requires observable viruses for filmic effect ▮

## AOL be Back

Dr Alan Solomon, founder of the software house sold last year to *NAI*, has been publicly touting for an anti-virus program to recommend to those with (suspected) on-line ailments. Solomon suggested that an earlier arrangement with the company he once owned, to supply regular trial copies of *Dr Solomon's FindVirus*, (the scanner from the *AVTK*) has fallen victim to the *NAI* takeover.

Posting in the Usenet newsgroup alt.comp.virus, Solomon emphasized the large *AOL* userbase which forms the potential audience for his Safety Online forum hosted by the service provider. Detection of AOL Trojans was listed as a necessity, and respondents claiming to represent *iRiS*, *Symantec* and *Trend Micro* were seen publicly clamouring to have their products so honoured ▮

## Russian Excel-ence?

*Finjan*, the self-proclaimed 'founder and leader of the Internet mobile code security market', hit the news early this month. The Israeli company claimed to have uncovered 'an extremely dangerous security hole that could effect virtually anyone surfing the Internet'.

As has been remarked before, claims of 'discovery' in the anti-virus and security worlds are best treated with a healthy slice of skepticism. In this case, it was justified. The *Finjan* press release and associated brouhaha it raised were little more than thinly disguised publicity. Reading the press release carefully, *Finjan* was not claiming to have discovered this 'problem'.

In fact, it was discovered sometime in November by researchers at *Kaspersky Lab*. This is hinted at in *Finjan's* publicity, where it is referred to as the Russian New Year Exploit. *Kaspersky Lab* reported its findings to *Microsoft*, which set about working on a fix.

The 'exploit' consists of two parts. When combined they can allow code from a remote server to run on the browsing machine without the customary warnings. The web browser part depends on a wrinkle in the browser's rules for warning of possibly executable content. There are HTML constructs that cause some browsers to download a remote spreadsheet (or other files) *and* load it into *Excel* for display, without warning of the security violation.

The *Excel* component of the exploit depends on the CALL command. If not run from a macro, and the file contains no macros or customizations, *Excel* does not warn that code may be about to run (as in the typical macro warning case) when there are CALL statements present. Kaspersky Lab has demonstrated a simple COM dropper exploit with this.

*Microsoft* has posted updates for both *IE* and *Excel 97* to address these shortcomings. The *Excel* patch only installs over SR-2. It is unclear whether an *Excel 95* fix is likely ▮

## VB Vacancy

*Virus Bulletin* is currently seeking a technical consultant for an immediate start at its Abingdon office. The ideal candidate must possess a good knowledge of computer viruses, web design (HTML), and popular operating systems and networks. A working knowledge of *Adobe PageMaker* and the *Microsoft Office* application suite would be an advantage.

Working closely with the Editor, duties include all the in-house product testing and comparative review procedures from liaising with anti-virus developers to the production of finished copy, maintenance of the *VB* web site, and compilation of the monthly prevalence table. This position also supplies technical support for *VB* subscribers. For more information contact *Virus Bulletin*; tel +44 1235 555139, fax +44 1235 531889, or email editorial@virusbtn.com ▮

# IBM PC VIRUSES (UPDATE)

The following is a list of updates and amendments to the *Virus Bulletin Table of Known IBM PC Viruses* as of 15 December 1998. Each entry consists of the virus name, its aliases (if any) and the virus type. This is followed by a short description (if available) and a 24-byte hexadecimal search pattern to detect the presence of the virus with a disk utility or a dedicated scanner which contains a user-updatable pattern library.

**Type Codes**

| | | | |
|---|---|---|---|
| **C** | Infects COM files | **M** | Infects Master Boot Sector (Track 0, Head 0, Sector 1) |
| **D** | Infects DOS Boot Sector (logical sector 0 on disk) | **N** | Not memory-resident |
| **E** | Infects EXE files | **P** | Companion virus |
| **L** | Link virus | **R** | Memory-resident after infection |

**Acy.790**

**CN:** An appending, 790-byte, direct infector with the texts 'ACY corp. Omsk Sity, Russia,USSR' and 'Hello for PC WORLD, Interquadro,ParaGraf !'. Infected files' time-stamps are set to four seconds.

```
Acy.790             B96F 0032 C0F3 AA8D 9663 FDB4 40B9 1603 CD21 7213 5A59 83E1
```

**Adri.886**

**ER:** An encrypted, appending, 886-byte virus containing the text 'f-tbvichscclnaF-TBVICHNASCCL'.

```
Adri.886            BF?? 00B4 ??B9 7603 2E8A 0581 FF?? 0072 0532 C42E 8805 D0C4 02E0 47E2
```

**ByteWarrior.1214**

**CN:** An encrypted, appending, 1214-byte virus containing the texts 'This is an illegal copy.', '—> BYTE WARRIOR GOTCHA! <—', 'BYTE WARRIOR says: We spit on those who choose to pose and trash with all the rest. Your Harddisk(s) had choosen to pose ... now they are trashed like the rest!', '*.COM' and 'PATH='. Infected files have their time-stamps set to four seconds.

```
ByteWarrior.1214    8104 BA?? ??BF ???? 8BEF 8A05 4D8A 6600 2AE0 8866 00E2 F5FC
```

**Enculator.1833**

**CEN:** An appending, 1833-byte, direct infector containing the texts 'ENCULATOR III', '*.COM', '*.EXE', 'COMSPEC=', 'SMARTCHK.*' and 'CHKLIST.*'.

```
Enculator.1833      B440 B924 07BA 0001 03D5 3E8B 9E14 013E 899E 1201 3E8B 9E36
```

**Fairground.813.B**

**ER:** An encrypted, 813-byte appender containing the texts 'BY [A319],HUNGARY ', 'CATE V@' and ' VARIANT !'.

```
Fairground.813.B    81C3 3E00 B9ED 028A 07E8 0800 8807 43E2 F61F EB12 5053 51B8
```

**Grubyc.1100**

**CR:** An appending, 1100-byte virus containing the encrypted text 'CYBURG1 (Chronophage) - Beta Release 1994 ! Special Thanks to : HA HA High Technology. Remember : Some Human Actions Have Real Artistic Mysteries... Cyburg'. Infected files have their time-stamps set to 62 seconds.

```
Grubyc.1100         8005 0547 E2FA B94C 04BA 0000 E838 00BF EB01 B9A0 009C 802D
```

**GW.1000**

**CER:** An encrypted, appending, 1000-byte virus containing the text 'AIDSDRWECOMM'. Infected files have the byte 11h at offset 0003h (COM) and 0012h (EXE).

```
GW.1000             5F47 572E A0E5 00B9 0203 BBE6 00E8 0100 C32E 3007 43E2 FAC3
```

**Hardcore.2123**

**CN:** A prepending, 2123-byte, direct infector which infects one file at a time. It has the encrypted texts 'All of this is Happy Hardcore:' and 'GFX by Demon'97'. The virus reinfects infected files.

```
Hardcore.2123       B440 8B1E E706 B94B 0890 32ED BA3E 07CD 21BA FA06 B45B B902
```

**Jak**

**CN:** Two direct infecting appenders with the texts '*.com' and '[Jerk1N / DIFFUSION]'. The 211-byte variant also has the text '[JaK.Parasitic]' and the 254-byte variant '[JaK.Parasitic.Crypt]'. They both reinfect infected programs.

```
Jak.211             B440 B9D3 008D 9603 00CD 21E8 0100 C3B4 3ECD 21C3 B43D B002
Jak.254             E836 FF5B B440 B9FE 008D 9603 00CD 2153 E826 FF5B E803 00C3
```

**Jak.120**

**CN:** An overwriting, 120-byte, direct infector with the texts '*.com', '[JaK.Small]' and '[Jerk1N / DIFFUSION]'.

```
Jak.120             E816 0072 B8B4 40B9 7800 8D96 0000 CD21 E801 00C3 B43E CD21
```

**Jak.144**

**CN:** An overwriting, 144-byte, direct infector containing the texts '*.com', '[JaK.Stealth]' and '[Jerk1N / DIFFUSION]'. Infected files start with the word 4B50h ('PK') – similar to ZIP archives.

```
Jak.144             E816 0072 B6B4 40B9 9000 8D96 0000 CD21 E801 00C3 B43E CD21
```

**Jak.196**

**CN:** An encrypted, overwriting, 196-byte, direct infector containing the texts '*.com', '[JaK.Crypt.Stealth]' and '[Jerk1N / DIFFUSION]'. Infected files start with the word 4B50h ('PK').

```
Jak.196             E886 FF5B B440 B9C4 008D 9600 00CD 2153 E876 FF5B E801 00C3
```

**Jerkin.439**

**CN:** An encrypted, appending, 439-byte virus with the texts '*.c?m', '[Lone.Vengance]', '[J1N/D]', 'I hate doin this but I was asked to take you down!', 'Next time you will loose ALL your data!' and 'Jerk1N, of DIFFUSION].

```
Jerkin.439          EFE8 0200 EB12 B9BA 008D 9E2C 008B 96B8 0131 1743 43E2 FAC3
```

**Jerkin.521**

**CN:** An encrypted, appending, 521-byte virus containing the text '[JVS 1.3]' and the encrypted messages 'Happy Birthday Kellie, From Jer' and '[Kellie.B] [Jerk1N/DIFFUSION]'.

```
Jerkin.521          53B9 1B00 8D9E 9A01 8B86 F801 3107 4343 E2FA 5BC3
```

**Kampi.4181**

**CER:** An appending, 4181-byte virus, containing the texts '20:38:07, 8-09-98,' and 'Warning : ONLY FOR PRIVATE USE'.

```
Kampi.4181          E83D 00C3 BA00 01B9 5510 B440 E841 FEC3 B802 4233 C933 D2E8
```

**Moskau.846**

**CN:** An encrypted, appending, 847-byte virus containing the texts '<MOSKAU98>Stas' and *.com'.

```
Moskau.846          B440 B94E 0390 8BD5 CD21 8BF5 81C6 7201 8CC8 CD01 8BFC 8B75
```

**Munya.517**

**CN:** An appending, 517-byte, direct infector with the text '????????COM'. Infected files have the byte 2Ah ('*') at offset 0003h. The payload clears the lower byte of the Base Memory size stored in CMOS registers (ie, on a machine with 640 KB of conventional memory, the payload resizes it to 512 KB).

```
Munya.517           C684 0903 2AB4 40B9 0400 8D94 0603 CD21 B43E CD21 B801 438D
```

**Mutant.1778**

**CER:** A mildly polymorphic, 1778-byte appender containing the texts 'COM.EXE.com.exe' and '* MUTANT-93 * (Pre-Release version).'. The following template detects the virus in memory only.

```
Mutant.1778         30C0 CF3D DDDD 742A 3D00 4B74 3480 FC11 7427 80FC 1274 2280
```

**Nop.355**

**CN:** A prepending, 355-byte, direct infector containing the texts 'NOP', '*.COM' and '????????COM'.

```
Nop.355             B440 BA00 01B9 6301 CD21 7263 B43D BA54 02B0 00CD 2172 582E
```

**Opic.1716**

**CEN:** An encrypted, appending, 1716-byte virus containing the texts 'Prospero Virus(C) Opic [CodeBreakers '98]' and '**********PROSPERO!********** There is a path to the trancendece of the dollar: Embark rich beggars! Does magic bring prosperos to his knees? Reading pretty twilight, making grass uncertain? Oh,all that christmas snow shouldered by one birthday suit! The fate of the world under his armpit like a thermometer? Rejoice Villains! Your time has come. **********(C) Opic [CodeBreakers,98]**********'. The virus is mildly polymorphic and uses a table-driven polymorphic engine. The following templates cover all possible replicants.

```
Opic.1716           E800 00FB 5D93 81ED 1001 8DB6 3C01 8BFE B983 06E8 0400 EB17
Opic.1716           E800 0058 9393 2D10 0195 8DB6 3C01 8BFE B983 06E8 0400 EB17
Opic.1716           E800 0090 5890 2D10 0195 8DB6 3C01 8BFE B983 06E8 0400 EB17
Opic.1716           FAE8 0000 58FB 2D11 0195 8DB6 3C01 8BFE B983 06E8 0400 EB17
Opic.1716           FCE8 0000 5DF8 81ED 1101 8DB6 3C01 8BFE B983 06E8 0400 EB17
Opic.1716           FB90 E800 005D 81ED 1201 8DB6 3C01 8BFE B983 06E8 0400 EB17
Opic.1716           FBF8 E800 0058 2D12 0195 8DB6 3C01 8BFE B983 06E8 0400 EB17
```

**Prodigy.268**

**CN:** An overwriting, 268-byte direct infector containing the texts '*.COM', 'Pr0diGy VeEr0oZ (c) 1995' and 'HaPpY nEw YeAR! SeE U iN HeLL...'.

```
Prodigy.268         890E C301 8916 C101 BA00 01B4 40B9 0C01 CD21 90B8 0157 8B16
```

**Saha.2382**

**CR:** An overwriting, 2382-byte virus which infects COM files and modifies EXE files with the same name as COM targets. The virus appends nine bytes (the string ' Sahand ') to EXE programs.

```
Sahand.2382         B918 048D 1618 058B 1EBF 09B4 40CD 21B9 8F00 8D16 3009 8B1E
```

**Simple.331**

**CN:** An encrypted, appending, 331-byte, direct infector with the text '*.COM'. Infected programs ends with the string 'SIMPLE'.

```
Simple.331          60E8 0000 5E81 EE32 01B9 2E01 2EF6 1446 E2FA 61C3 5349 4D50
```

**Spartak.1360**

**CEN:** An encrypted, appending, 1360-byte virus containing the texts 'COWIIBAIAVDRWEADHICH', 'Spartak Virus by Crazy Punk (C) | v1.0 beta', 'Moscow, Russia, 06/10/1998', 'F_C_S_M.COM', '*.com' and '*.exe'. The last two bytes are XOR-ed together give the value of 0FFh.

```
Spartak.1360        B919 031E 06E8 0000 FA5D 81ED 0E01 0E1F BA40 0052 07B8 ????
```

**Spartak.1453**

**CEN:** An encrypted, appending, 1453-byte virus with the texts 'COWIIBAIAVDRWEADHICH', 'Spartak-II Virus by Crazy Punk (C)', 'Moscow, Russia, 06/10/1998', '*.com' and '*.exe'. The last two bytes are XOR-ed together give the value of 0FFh.

```
Spartak.1453        1EB9 4804 06BA 4000 E800 00FA 5D81 ED11 010E 1F52 07B8 ????
```

**Spy.447**

**CN:** A 447-byte appender with the texts 'host.com', 'Opening file:', 'Unable to open file.', 'Storing first three bytes:', 'Storing file size...', 'Appending virus code...' and 'Setting jump to virus code...'.

```
Spy.447             B440 B9BF 018D 9600 01CD 21C3 8D9E 9E02 E82D 008B 8601 012D
```

**Variola**

**MDR:** An boot sector virus which infects MBRs on hard disks and DOS Boot Sectors on diskettes. It has the encrypted text 'PeaceMaker by VaRiOLa'. The virus stores the original boot sectors encrypted.

```
Variola             8BD9 D1E9 4B8A 248A 0032 E132 C126 8805 2688 2146 474B E2EC
```

**Wild.2406**

**CER:** An appending, 2406-byte virus.

```
Wild.2406           B873 0BBB 7373 CD21 80FC 7374 03E9 6B08 0E58 1E5B 2BC3 7518
```

**XM.2401**

**CE:** A polymorphic, 2401-byte appender with the texts '[XyeBo_MHe], (c)MidnighÅPr0wler - =Version', 'COMMAND.COMDOS4GW.EXEIBMBIO.COMCOMEXEcomexe' and 'c:\autoexec.bat'. Infected files have the word E958h at offset 0000h (COM) and the word FAFAh at offset 0010h (EXE). The following template detects the virus in memory only.

```
XM.2401             B961 0953 E80E FE5B 2E89 0E1E  0406 1FB4 BFBA 1C00 E862 FAE
```

# VIRUS ANALYSIS

## Parvo – One Sick Puppy?

*Péter Ször*
*Data Fellows*

Typically, hoax warnings are scare alerts started by malicious people and passed on by innocent users who think that by spreading the warning they are helping the PC community. We have seen cases where email systems have collapsed after dozens of users forwarded a false alert to everybody in the organization.

Now there is a new virus called Win32/Parvo.A. It is capable of sending hoax emails with infected attachments. Parvo is a so-called 'research' virus – one that has not been reported from the field yet, but whose techniques could raise a serious issues if adopted by others. It is based on Win95/Marburg.A, but is more advanced.

Parvo is the first virus with a real communication module inside its 15 KB of assembler-written code. The virus can communicate with news and mail servers by using socket communication. When Parvo activates it emails dial-up information to the virus writer who can use it to break into networks. It replicates on *Windows 9x* and *NT*, and its polymorphic engine is a bit more complex than the one used in Marburg. Thus, Parvo is the first assembly-written polymorphic virus to work under *NT*.

### Initialization

Parvo is a PE infector. When an infected application is executed the virus takes control. When the host program does not have a relocation affecting the first five bytes at its entry point (EP) the virus places a jump instruction there, thus not modifying the EP field of the PE header. If there *is* a relocation for the first instruction at the EP, Parvo does not infect, leaving the EP entry in the header unchanged.

Parvo is tricky in the same way as Marburg. When there are no relocations for the first 255 bytes from the EP the virus not only places a jump instruction in the code at the entry point of the host, but builds a random garbage code block first and puts the jump to the virus polymorphic decryptor at the end of it. The size of the junk block together with the jump will be less than 255 bytes. The JMP instruction will point to the very end of the real virus body which is always attached to the last section of the host program. Infected files will grow around 15,000 bytes. Parvo pads itself to make the infected file size evenly divisible by 101 – the 29A group's 'standard' infection marker.

When the polymorphic decryptor finishes its work, the virus body is not yet completely decrypted. A second short decryptor is used for this. Then a checksum of the virus body is calculated and compared to the one saved during infection. In the case of a checksum mismatch, the virus simply terminates. This could be a precaution against its code being corrupted whilst being sent over the network.

If all is well, the virus looks for the base address of KERNEL32.DLL loaded into the virtual memory of the current process. This routine checks the *NT* DLL address space first, then that of *Windows 95* and gets the base of KERNEL32.DLL. Now the virus is able to get the address of the GetProcAddress API. The main difference here compared to other Win32 viruses is that Parvo does not employ API-name strings for this. Instead, it uses a technique similar to Win95/Voodoo, having pre-calculated checksums of their names. Thus, long strings do not take much space in the virus body. This makes analysis more time-consuming since all addresses it uses have to be checked during active debugging.

Parvo is interested in 36 APIs altogether (CreateFileA, CreateFileMappingA, … , GetTempPathA) and it gets all of them by calling GetProcAddress API in a loop. If an error occurs while doing this, the virus terminates. Otherwise, it allocates 132,605 bytes from the virtual memory of the process (more exactly 33 pages, 135,168 bytes, since the OS allocates memory in page-sized blocks), copies itself there, then passes control to that copy of the virus code. This mechanism is necessary because the polymorphic engine and the communication module need free memory.

### Operation at the Process Level

Parvo works in a similar way to a direct action infector, but stays in memory for a longer period because of its communication module. The virus is designed to infect fifteen different applications that typically execute for long periods of time, allowing it to complete those communications.

Parvo uses a new strategy in memory. After its initialization procedures run, the virus executes the host program as a child process while the virus runs as the process executed by the user. If, for instance, an infected copy of Netscape Navigator is executed, the virus runs as NETSCAPE.EXE while the original application will run as a different process with a random four character name such as JWRK.EXE. The virus process waits until the child process terminates, and only after that, terminates itself.

It is guaranteed that only one copy of Parvo is running at any given time. If a new infected process is executed, only the host program will be executed by the virus code and subsequently that copy of the virus will be passive. The virus creates a RAM semaphore – PARVOVIROSIS – for that purpose. This will be seen by other copies of the virus as they initialize, causing them to execute then terminate. This allows Parvo time to infect new files silently and communicate with mail and news servers.

The virus gets the name of the host program and copies it under a temporary name in the same directory. Then it maps this new image into memory, but only the original size (leaving out the virus code). After that, it 'disinfects' the host in memory by correcting the code at the image's EP with the information saved during infection. It unmaps the image, creating a clean host program. Then it executes the new, temporary image via CreateProcessA, with the command line parameters passed to the infected host.

When this process starts to run, Parvo uses the APIs CreateSemaphoreA and ReleaseSemaphore to set the PARVOVIROSIS semaphore. Later, when the polymorphic module, the infection module, the communication module and, optionally, the trigger module have been used, the virus calls the WaitForSingleObject API to wait until the original host program under the temporary name finishes its execution. Then Parvo frees its semaphore, deletes the temporary EXE file, and terminates itself.

### The Polymorphic Module

Parvo is a slow polymorphic virus. On most machines no more than one generation of its polymorphic decryptor is generated because the virus will not infect more than a few files. This makes generating good sample sets for detection tests a bit more difficult. Goat files have to be renamed first to a file name that the virus will infect and then the virus executed again and again.

After executing the original program the polymorphic module is called to create a new polymorphic decryptor for the subsequent infections. The polymorphic engine uses different encryption methods and key sizes. It uses byte, word and dword-based keys with many different standard encryption methods, much like Marburg.

### Infection Module

When searching for files to infect, initially Parvo looks for the standard web browser and mail program recorded in the registry. Since registry-related APIs are not stored in KERNEL32.DLL, the virus has to load ADVAPI32.DLL and obtain the addresses of three APIs – RegOpenKeyA, RegQueryValueA and RegCloseKey – from it.

Then it uses these to retrieve the program names under HKLM\SOFTWARE\Classes\htmlfile\shell\open\command and HKLM\SOFTWARE\Classes\mailto\shell\open\command and tries to infect EXE files in those programs' directories. Parvo does not infect a program if its size can be divided by 101 without remainder.

After checking the file's size, Parvo computes the checksum of the file name and compares it to fifteen stored values. Thus, it will only infect EXE files whose names match CUTFTP32, IEXPLORE, INSTALL, INSTALAR, MSIMN, NETSCAPE, NOTEPAD, NTBACKUP, ORDER, RASMON, SETUP, TELNET, WAB, WABMIG or WINZIP32. If the name matches any of these the virus tries to infect the application. At first Parvo creates a new temporary name with other than an EXE extension (possibly to avoid some behaviour blockers that look for writes to EXEs), renames the file and maps it into memory. Then it calls its main infection subroutine.

This routine checks if the application is a *Windows* program, a 386 executable image, but not a DLL and that the last section is not shared. If all these conditions are met, Parvo tries to infect the file. First, it checks the relocations at the EP and makes modifications there accordingly. Then it checksums the actual virus body and saves this value into the initialization routine.

After that, it encrypts its virus body with the selected encryption method and places the decryptor together with the encrypted image into the last section of the host. The size of file will be padded to be divisible by 101. It adjusts the header to account for the new size of the host section and sets this section to be writeable. Thus, Parvo does not modify more than one field of the PE header, the size of image field. This is simple and elegant, *and* it calculates this field correctly. After that it unmaps the temporary image, sets the file time and attributes to their original values, then renames the file back to that of the host.

When both the mail and the web browser directories have been checked for infectible files, the virus first uses the FreeLibrary API to remove ADVAPI32.DLL from its process address space. Then it looks for other files to infect in the current directory, the *Windows* directory and the *Windows* system directory respectively using the same filename checksum-matching conditions described above.

### Communication Module

After the infection module, the communication module is called. At first this module loads WSOCK32.DLL and obtains the addresses of ten APIs from it (WSAStartup, inet_addr, gethostbyaddr, htons, socket, connect, send, recv, closesocket and WSACleanup). If all these addresses are available the virus loads RASAPI32.DLL and obtains the addresses of three APIs from it (RasEnumConnectionsA, RasEnumEntriesA and RasGetEntryDialParams). Otherwise it returns from the communication module.

Should the communication module continue to run, it first calls RasEnumConnectionsA. If this function fails, RAS (Remote Access Service) is not installed and/or there are no active RAS connections. In such cases, the communication module terminates and frees the two loaded DLLs from the process. After this, the virus selects a hoax message from a selection of three (Hoax A, B or C). It prepares the hoax message email header by filling the Subject:, Mail from and From: fields with the related values. However, the To: and Rcpt to: fields are filled randomly. The virus has to locate available email addresses from somewere to be able to fill these fields and spam someone. This is why Parvo tries to connect randomly to one of two possible Spanish Usenet (NNTP) news servers.

(I have to note here that these servers are not available to everybody, at least I do not have permission to use them. They may be out of order.) It connects to port 119 (NNTP) of the server then starts to communicate with it. There are three possible lists of news group names related to the three possible hoaxes.

Hoax A is related to various 'hacker' and 'cracks' groups. Hoax B is related to much the same list as Hoax A, but less the the last five entries. Hoax C is related to some 'erotica' and 'binaries' groups.

The virus uses the 'group' command with a randomly selected newsgroup name chosen from the list related to the hoax message it has selected. For instance, the virus selects Hoax B ('New and even larger serial number list out now!') and randomly selects the alt.binaries group name. Then it sends a 'group alt.binaries' command to the news server. That way this group becomes the active one to read. The news server will answer this message with the number of messages in that newsgroup. Then the virus repeats the 'head' and 'next' commands a random number of times.

Finally, Parvo searches for the 'From:' string in the buffer, picking out the poster's address. It puts this string after the 'To:' and 'Rcpt to:' fields of the prepared email header. Then the message is ready to be posted. Parvo disconnects from the news server and connects to port 25 (SMTP) of a randomly selected server from a list of six. Parvo's first message is 'helo' for the mail server with three different parameters: microsoft.com, quicknet.com or hoteens.com according to the selected hoax message. This is the standard way of introducing itself to the mail server. Then it sends the header of the email message field by field.

After that, Parvo creates a temporary file name with an EXE extension in the *Windows* TEMP directory. It fills the EXE file with a do-nothing PE host program. This image is placed in the virus body in compressed format. All the zero bytes are compressed as blocks of bytes. This makes the host program much shorter in the virus body.

Parvo then infects this file with the standard infection routine and uses the polymorphic decryptor and encryption prepared beforehand. It sets the original entry point data to C3h (RET) which will be used to 'disinfect' the image. That way this application will do nothing but execute the virus code. When the image is available Parvo sends a MIME header and after that a MIME64 encoded copy of the 20,503 byte file it has just prepared. Finally, it deletes this temporary file, leaves the server with the 'quit' command and frees the used DLLs from its process space.

The mail server will post the hoax message, with the infected attachment, to the selected person. The name of the attachment is MSEFIXI.EXE in Hoax A, LSERIAL.EXE in Hoax B and HOTEENS.EXE in Hoax C. This idea is clearly an attempt to ensure that many recipients of the hoax and attachment will be interested in executing the 'patch' program, thus infecting their PC.

### Trigger Module

When Parvo returns from the communication module it randomly calls up the final module – the trigger. The virus reconnects to one of the six possible email servers and randomly selects one of four possible email addresses – XTRO001@lycosmail.com, xtro002@lettera.net, XTRO004@usa.net or XTRO007@mailexcite.com. It prepares an email message to that address, apparently from lamer@lamer.net, and starts to send the mail header information to the server.

Then the virus uses the RasEnumEntriesA API and on all possible entries calls RasGetEntryDialParamsA in a loop. That way it posts mail including the following fields: Name:, Phone:, Callback:, Username:, Password:, Domain: of all entries from the dial up database. If the user saved their password into this database the hash of this password will be posted to the virus writer's email address. Password protection is known to be ineffective on *Windows 95* which means that attackers can use it to break into a network. When the mail is posted the virus disconnects from the mail server and waits for the executed child process to terminate.

### Conclusion

Win32/Parvo.A shows that virus writers are looking for new, faster methods to spread their creations over networks. We may see many viruses doing similar things during 1999 and unfortunately such viruses have the potential to spread much faster than most other virus types. We have to be ready for that to happen.

Prepare more serious policies against passing hoax messages inside and outside the company. Teach your users to not click on executable attachments even if the message is apparently from microsoft.com. Do not use functions which save your passwords anywhere in any form even if this speeds up your work a little!

## Win32/Parvo

| | |
|---|---|
| Aliases: | None known. |
| Type: | Win32 per-process resident, PE infector. |
| Self-recognition in Files: | Files whose size can be divided by 101 without reminder are assumed to be infected. |
| Hex Pattern in PE files: | Not possible, the virus is polymorphic. |
| Payload: | Sending out RAS user information, including passwords, to the virus writer's email address. |
| Removal: | Recover infected files from backup or replace with original. |

# COMPARATIVE REVIEW

## Competidores DOS

Compared with that of the February 1997 comparative, the line-up in this review is somewhat depleted. This is largely explained by the major anti-virus vendor barndance in the second half of 1997, meaning that *IBM* and *Dr Solomon's* no longer produce their own scanners.

Aside from that, while some regularly submitted products were not forthcoming, this review sees the return of *FRISK Software's* shareware *F-PROT* to *VB* reviews after representation by its various commercial incarnations for several years. The typical 'lottery' of the smaller developers – who seem to pick and choose their reviews – made up the balance of the sixteen products considered below.

In the preamble to that previous DOS comparative, it was noted that some developers were still shipping a separate macro virus scanner. While this still holds, all products reviewed herein have a standard scanner which detects macro viruses with the macro-only offering being an adjunct – perhaps as a matter of habit from those bygone days or as a *Windows* program, providing the user with a 'nicer', or at least more familiar, interface.

Recent months have seen a large increase in the use of polymorphism in macro viruses, and also the rise of the so-called 'class infector'. The latter is a form of *Word 97* macro virus that embeds its code in the default document stream in the OLE document file, rather than in its own module stream. This required many vendors to modify their macro virus detection routines.

Many class infectors were seen in the months and weeks leading up to the 26 October 1998 submission date for this comparative review, and as a large family of them (imaginatively named W97M/Class) combines this infection technique and polymorphism, a number of these were included in the viruses added to the usual *VB* test-sets.

Although no class infectors were listed on the October WildList (to which the In the Wild test-sets were updated) there have been clear indications of class infectors spreading successfully (see the News story, p.3 this issue), so effectiveness in detecting these new viruses is worth noting in the results.

### Test Procedures

Speed tests in this review were carried out on a standalone workstation. Detection tests were facilitated by storing the virus test-sets in a read-only directory on a *NetWare* server with the tests run from a series of batch processes launched from the server's login script. The workstations were programmatically reset at the conclusion of each product's test-run, automatically logging in after the restart and seeking out the next product to test. Measures used in previous *VB* DOS comparatives to test samples individually were deemed too resource-intensive with the increasing size of the test-sets employed.

Where a product offered the choice between a command-line and a menu-driven scanner, the former was always used. All products tested provided this choice or had an option for driving the product non-interactively. Default scanner settings were used as far as possible, except that reporting was always enabled and if it was not the default behaviour, all tested files were logged.

Speed tests were conducted against a selection of clean files on a local hard drive. This most closely reflects 'typical' operation in the real world. The Clean test-set consists of 5500 executables, comprising approximately 540 MB. The contents have been culled from common DOS and *Windows* applications, and from publicly accessible collections of freeware and shareware utilities. As well as being a speed test, this doubles as a false positive test – there are no viruses in this collection, so none should be found.

Lastly, two diskettes, each holding 26 EXE and 17 COM files, were used to test diskette scanning speeds. On one diskette the files are clean, and on the other, the same files are infected with Natas.4744.

### Alwil AVAST! v7.70.22 26 Oct 1998

| | | | |
|---|---|---|---|
| ItW Boot | 100.0% | Macro | 94.5% |
| ItW File | 99.6% | Polymorphic | 97.4% |
| ItW Overall | 99.6% | Standard | 99.7% |

A typically solid performance from *Alwil's AVAST!*, detecting all ItW boot viruses and samples of all ItW file viruses. Its downfall on the latter test-set is that, failing to scan SCR files (*Windows* screen savers) by default, it did not detect all samples of Win95/Marburg (see *VB*, November 1998, p.8) and TPVO.3783.A.

The VxD infector Navrhar was the only miss against the Standard test-set and the SCR and occasional EXE samples of Marburg accounted for the slightly less than perfect score against the Polymorphic set. Misses in the Macro test-set concentrated among the polymorphic, and particularly the newer class infectors.

The single-tasking nature of DOS means *AVAST!* may as well use the machine's full resources, rather than run as a low priority background thread (the approach of *AVAST32* for the *Windows* platforms). Returning a throughput rate of approximately 2 MB/s, *AVAST!* demonstrates that the core engine is no slug. No false positives occurred.

| On-demand tests | ItW Boot | | ItW File | | ItW Overall | Macro | | Polymorphic | | Standard | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Number | % | Number | % | % | Number | % | Number | % | Number | % |
| Alwil AVAST! | 82 | 100.0% | 726 | 99.6% | 99.6% | 2483 | 94.5% | 14189 | 97.4% | 1031 | 99.7% |
| Command AntiVirus | 79 | 96.3% | 738 | 100.0% | 99.6% | 2592 | 98.7% | 14438 | 99.1% | 1031 | 99.7% |
| Cybec Vet Anti-Virus | 82 | 100.0% | 721 | 99.0% | 99.1% | 2196 | 83.6% | 14035 | 96.2% | 1024 | 99.2% |
| Data Fellows FSAV | 82 | 100.0% | 738 | 100.0% | 100.0% | 2597 | 98.9% | 14415 | 99.8% | 1040 | 100.0% |
| DialogueScience Dr Web | 81 | 98.8% | 738 | 100.0% | 99.9% | 2463 | 93.7% | 14444 | 100.0% | 1028 | 99.5% |
| ESET NOD32 | 82 | 100.0% | 738 | 100.0% | 100.0% | 2580 | 98.1% | 14381 | 99.5% | 1039 | 99.7% |
| FRISK F-PROT | 79 | 96.3% | 738 | 100.0% | 99.6% | 2602 | 99.1% | 14444 | 100.0% | 1031 | 99.7% |
| Grisoft AVG | 80 | 97.6% | 721 | 98.3% | 98.2% | 1778 | 68.8% | 14290 | 98.1% | 1018 | 98.6% |
| H+BEDV AntiVir | 79 | 96.3% | 669 | 97.2% | 97.1% | 1913 | 74.2% | 11930 | 81.9% | 1008 | 97.9% |
| iRiS AntiVirus | 82 | 100.0% | 738 | 100.0% | 100.0% | 2359 | 90.0% | 14433 | 99.1% | 1040 | 100.0% |
| Kaspersky Lab AVP | 82 | 100.0% | 738 | 100.0% | 100.0% | 2596 | 98.6% | 14444 | 100.0% | 1040 | 100.0% |
| NAI McAfee VirusScan | 82 | 100.0% | 738 | 100.0% | 100.0% | 2575 | 98.2% | 14337 | 98.0% | 1040 | 100.0% |
| Norman ThunderBYTE | 82 | 100.0% | 729 | 99.6% | 99.7% | 2448 | 93.8% | 14023 | 95.4% | 1014 | 98.8% |
| Norman Virus Control | 82 | 100.0% | 738 | 100.0% | 100.0% | 2455 | 94.0% | 14294 | 99.0% | 1031 | 99.7% |
| Sophos Anti-Virus | 82 | 100.0% | 738 | 100.0% | 100.0% | 2409 | 92.2% | 14444 | 100.0% | 1021 | 99.2% |
| Symantec Norton AntiVirus | 82 | 100.0% | 738 | 100.0% | 100.0% | 2607 | 99.1% | 14443 | 98.7% | 1036 | 99.7% |

## Command AntiVirus v4.52 19 Oct 1998

| | | | |
|---|---|---|---|
| ItW Boot | 96.3% | Macro | 98.7% |
| ItW File | 100.0% | Polymorphic | 99.1% |
| ItW Overall | 99.6% | Standard | 99.7% |

This is the first *VB* test of *Command Software AntiVirus* (*CSAV*) for DOS based on the v3.x *FRISK* engine. Despite submitting a product with a scan string file dated 1 August, *CSAV* detected 100% of the ItW file samples. Three ItW boot infectors were missed, however – ones that have caused problems for others in the past – EXEBug.Hooker, Michelangelo and Quox.

The Navrhar VxDs and six samples of Cryptor.2582 were all that stood between *CSAV* and full detection of the Standard and Polymorphic test-sets respectively. Despite the relatively old SIGN.DEF file already mentioned, the equivalent file of macro virus identification data was dated 19 October. This, no doubt, accounted for the impressive 98.7% detection rate against the Macro test-set, which was only marginally bettered by three other products. Hard disk scanning speed is quite acceptable with a throughput just short of 2 MB/s.

Surprisingly for *CSAV*, one 'suspicious' file was found in the Clean test-set. The log produced from that run commented upon two files (one 'could be corrupted' and another 'could be destructive'). As files from the virus test-sets classed as 'suspicious' were counted as detections, this has to count as a false positive.

## Cybec Vet Anti-Virus v9.90 20 Oct 1998

| | | | |
|---|---|---|---|
| ItW Boot | 100.0% | Macro | 83.6% |
| ItW File | 99.0% | Polymorphic | 96.2% |
| ItW Overall | 99.1% | Standard | 99.2% |

Detecting all the ItW boot samples was a good start, but *Vet's* failure to scan SCR files by default partly accounts for it missing a VB 100% award. The polymorphic macro virus W97M/Groov.B also played a part in this.

Similar factors largely accounted for *Vet's* misses against the Polymorphic test-set, with Marburg-infected SCRs and macro viruses XM/Compat, Groov.B and W97M/Splash.A taking their toll. As with several products in this review the Navrhar VxDs largely accounted for misses in the Standard

| | Scanning Speed | | | | | | False Positives |
|---|---|---|---|---|---|---|---|
| | Diskette - Clean | | Diskette - Infected | | Hard Drive - Clean | | |
| | Time (seconds) | Throughput (KB/s) | Time (seconds) | Throughput (KB/s) | Time (min:sec) | Throughput (KB/s) | |
| Alwil AVAST! | 40 | 24 | 81 | 15 | 4:18 | 2070 | 0 |
| Command AntiVirus | 32 | 30 | 38 | 31 | 4:41 | 1901 | 1 |
| Cybec Vet Anti-Virus | 38 | 26 | 39 | 30 | 2:03 | 4342 | 1 |
| Data Fellows FSAV | 50 | 19 | 39 | 30 | 23:00 | 387 | 2 |
| DialogueScience Dr Web | 77 | 13 | 62 | 19 | 53:16 | 167 | 19 |
| ESET NOD32 | 34 | 29 | 45 | 26 | 2:41 | 3317 | 0 |
| FRISK F-PROT | 32 | 30 | 37 | 32 | 4:10 | 2136 | 1 |
| Grisoft AVG | 53 | 18 | 62 | 19 | 8:57 | 995 | 10 |
| H+BEDV AntiVir | 47 | 21 | 55 | 21 | 3:31 | 2531 | 2 |
| iRiS AntiVirus | 41 | 24 | 35 | 34 | 7:55 | 1124 | 1 |
| Kaspersky Lab AVP | 51 | 19 | 39 | 30 | 22:45 | 391 | 2 |
| NAI McAfee VirusScan | 46 | 21 | 55 | 21 | 5:09 | 1729 | 0 |
| Norman ThunderBYTE | 28 | 35 | 31 | 38 | 1:28 | 6069 | 0 |
| Norman Virus Control | 53 | 18 | 55 | 21 | 5:10 | 1723 | 16 |
| Sophos Anti-Virus | 46 | 21 | 36 | 33 | 7:49 | 1139 | 0 |
| Symantec Norton AntiVirus | 45 | 22 | 47 | 25 | 8:05 | 1101 | 0 |

test-set. Results against the macro test-set were disappointing. With a definitions file dated 20 October, better detection of the newer viruses added to the test-set for this review was expected.

As usual, *Vet* was very near the top of the speed chart, although its throughput is noticeably lower than in the February 1998 DOS comparative. One false positive for an HLL virus was reported.

## Data Fellows FSAV v3.0.125 24 Oct 1998

| | | | |
|---|---|---|---|
| ItW Boot | 100.0% | Macro | 98.9% |
| ItW File | 100.0% | Polymorphic | 99.8% |
| ItW Overall | 100.0% | Standard | 100.0% |

*Data Fellows' F-Secure Anti-Virus* attained VB 100% level performance against the combined ItW test-sets. Unlike *FSAV* for most other platforms, which combine the *FRISK* and *Kaspersky Lab* engines, the DOS incarnation of *FSAV* uses just the latter.

Detecting all the samples in the Standard test-set does not leave much room for comment. Most of the small number of macro viruses missed were those most recently added to the test-set. Detecting all but 21 of the 50 XM/Compat.A samples in the Polymorphic set and none of the eleven in the Macro test-set will require improvement if the *NT* product is to obtain a VB 100% award in the upcoming March comparative. This virus made it to the December 1998 WildList which will be the basis of the ItW File test-set used for that review.

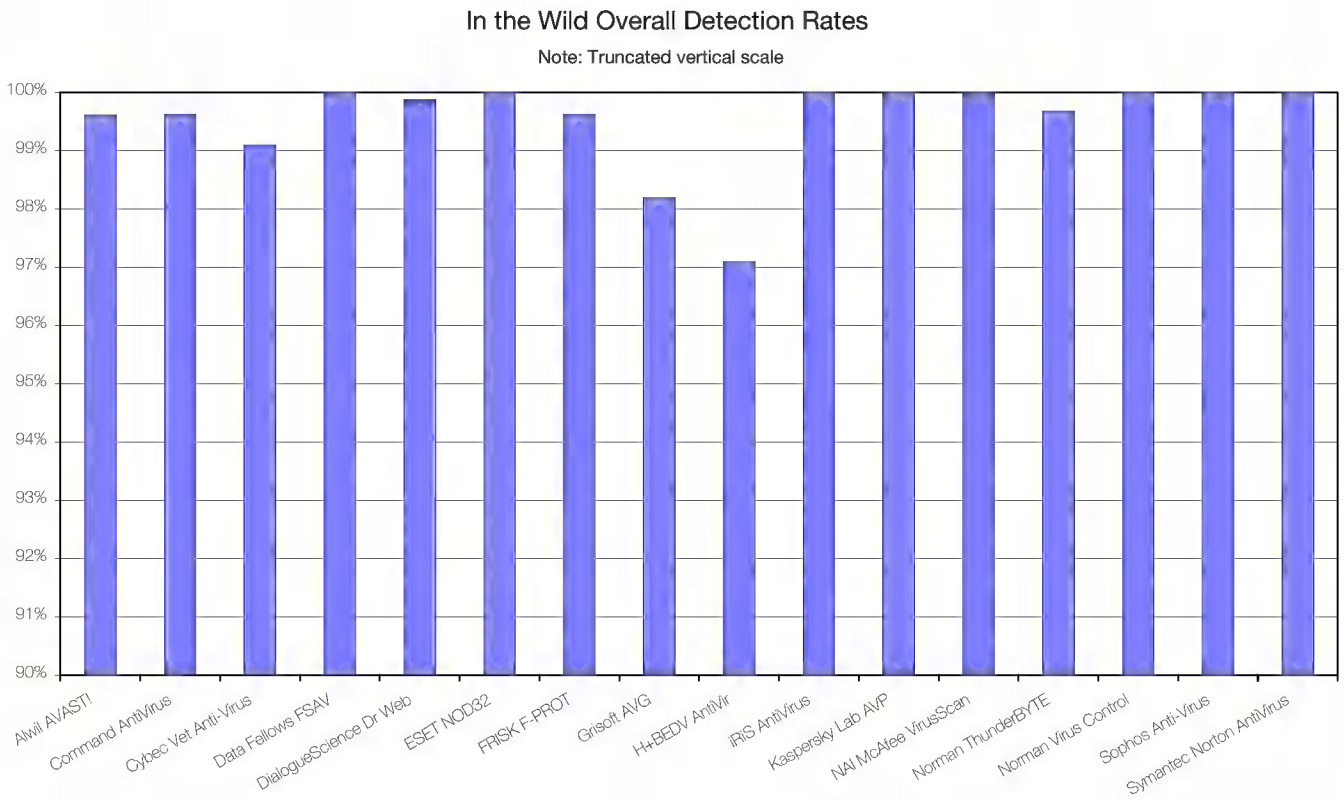
The *AVP* engine is unlikely to be accused of high speed, and with a throughput slightly below 400 KB/s, this incarnation of it puts *FSAV* among the slowest three products. Suspicion of two 'Type_ComExeTSR' viruses in the Clean set is not unusual with products relying so heavily on emulators and heuristics, but is still undesirable.

## DialogueScience Dr Web v4.03 23 Oct 1998

| | | | |
|---|---|---|---|
| ItW Boot | 98.8% | Macro | 93.7% |
| ItW File | 100.0% | Polymorphic | 100.0% |
| ItW Overall | 99.9% | Standard | 99.5% |

Ornate from the ItW Boot set was the fly in the ointment which prevented *Dr Web* from achieving a VB 100% award. This is a notable improvement over the performance of *DialogueScience's* Win32 scanner against much the same Boot set in the November 1998 comparative.

Perfect detection of the Polymorphic test-set samples has been something of a *Dr Web* speciality and it was one of only four products to achieve that level of performance here. The MemLapse.289 and Navrhar VxD samples were missed in the Standard set and the misses in the Macro set were mainly the newest of viruses to be added to that set.




*Dr Web* seems destined to place slowest in *VB* Clean set speed tests and so it was in this review. As noted before, its near-glacial speed, resulting in a throughput of 167 KB/s, should be largely offset should it be used in association with *DialogueScience's* integrity checker. Nineteen false-positives is too many.

## ESET NOD32 v1.11

| | | | |
|---|---|---|---|
| ItW Boot | 100.0% | Macro | 98.1% |
| ItW File | 100.0% | Polymorphic | 99.5% |
| ItW Overall | 100.0% | Standard | 99.7% |

*ESET's* little-known (at least, outside its native Slovakia) *NOD* continues its recent impressive showings in *Virus Bulletin* comparative reviews, picking up a VB 100% award here.

Power_Pump.1 was the only virus to elude *NOD32* in the Standard test-set, and the small number of the most recently received macro viruses missed in that set demonstrates how up to date the product was in that quarter. Analysis of the samples of the only virus missed in the Polymorphic test-set (W97M/Splash.A) reveals a potential design limitation in *NOD32* – it does not seem to handle large macros well.

W97M/Splash.A morphs itself by randomly inserting randomly-generated comment lines into its code. This has no ill-effect on the virus but makes the VBA code and associated structures in the host document file larger with each generation. The *Virus Bulletin* Polymorphic test-set contains 100 replicants, randomly selected from a set of 517 samples generated so that each was larger than its forebear. *NOD32* stopped detecting Splash as the document approached 250 KB, although the limiting factor is most likely the size of some internal structure in the document under examination or perhaps resources available to the scanner, such as memory.

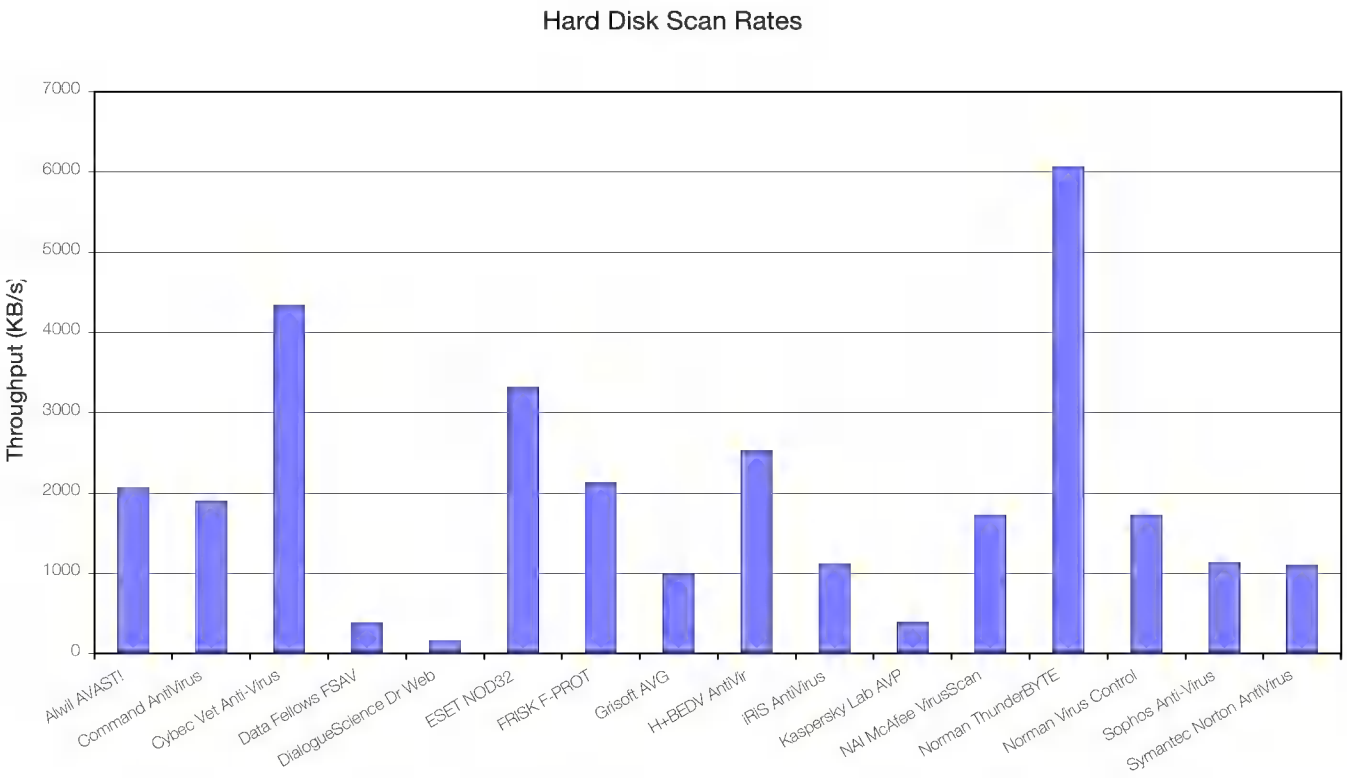
It is almost a truism in the anti-virus field that you can have speed or good detection. However, *NOD32* is one of the products that bucks that idea, effectively coupling the two. It returned the third highest throughput on the Clean test and did so without false alarm.

## FRISK F-PROT v3.03a 26 Oct 1998

| | | | |
|---|---|---|---|
| ItW Boot | 96.3% | Macro | 99.1% |
| ItW File | 100.0% | Polymorphic | 100.0% |
| ItW Overall | 99.6% | Standard | 99.7% |

The welcome return of *FRISK Software's F-PROT* to *VB* tests was not as triumphal as some may have expected. As with *CSAV*, three elderly and historical troublemakers in the ItW Boot test-set prevented *F-PROT* from turning in a performance worthy of a VB 100% award.

This similarity of perfomance should not be surprising, as the two employ the same engine. *F-PROT's* correct detection of all Cryptor samples is likely due to the more up to date SIGN.DEF file, with the five-day newer MACRO.DEF making the difference on the Macro test-set. Comments about other aspects of performance are the same as for the *Command* product.




## Grisoft AVG v5.0 (build 1234)

| | | | |
|---|---|---|---|
| ItW Boot | 97.6% | Macro | 68.8% |
| ItW File | 98.3% | Polymorphic | 98.1% |
| ItW Overall | 98.2% | Standard | 98.6% |

Missing ABCD and TPVO.3783.A from the ItW Boot set was not an auspicious start for *AVG*. However, then failing to detect three macro viruses from the In the Wild File set (WM/Nottice.A, WM/TWNO.AC and X97M/Extras.B) is probably not that surprising a result, as the Macro test-set was its weakest area of performance. With a detection rate lower than 70%, this must be an area of some concern, as in earlier *VB* reviews.

It is, however, encouraging to note *AVG's* marked improvement against the Polymorphic set where, apart from missing all X97M/Compat.A and W97M/Splash.A macro viruses, only four samples of Cryptor.2582 evaded *AVG*.

Ten false alarms against the *VB* Clean set is too many. This is especially so when five of them were against various different versions of Vernon Buerg's extremely popular, and therefore widely distributed, *List* utility and one against a version of *Microsoft's* DOS network client manager utility NET.EXE!

Scanning speed was neither remarkably fast nor grindingly slow, although nearer the latter. At approximately 1 MB/s, it was in the company of the products by *iRS*, *Sophos* and *Symantec*, although with those offerings the price of this somewhat pedestrian speed is offset by notably higher detection rates.

## H+BEDV AntiVir v5.15.0.8

| | | | |
|---|---|---|---|
| ItW Boot | 96.3% | Macro | 74.2% |
| ItW File | 97.2% | Polymorphic | 81.9% |
| ItW Overall | 97.1% | Standard | 97.9% |

Somewhat confusingly, two commandline scanners are included in the *H+BEDV* product – AVScan and AVE32. The results here are those produced by the latter, as it had the higher detection rate. In general these rates are much as they have been in recent reviews.

While the product missed three viruses in the ItW Boot set, these were not the 'usual three' mentioned elsewhere, but ABCD, Lilith and Moloch. The misses against the ItW File set were mainly the more recent polymorphic additions to the set, including Marburg.

The slight improvement over recent performances against the Polymorphic set is largely due to *H+BEDV's* detection of all samples of two of the three macro viruses, with the more complex polymorphic executable infectors still defeating it. The recently added class infectors and several of the other polymorphic macro viruses only represented in the Macro test-set collectively took their toll on *H+BEDV's* detection rate against this set. Improvement here must be considered urgent given the continuing proliferation of macro viruses.

With a throughput of 2.5 MB/s, *H+BEDV* placed fourth fastest against the Clean test-set. Although a creditable speed, overall, higher detection and removal of the two false positives is to be desired.


## iRiS AntiVirus v22.14 26 Oct 1998

| | | | |
|---|---|---|---|
| ItW Boot | 100.0% | Macro | 90.0% |
| ItW File | 100.0% | Polymorphic | 99.1% |
| ItW Overall | 100.0% | Standard | 100.0% |

Longtime participants in *VB* tests, Israeli *iRiSAV* has been putting some consistently high detection scores in recent tests, and in this comparative collected its second VB 100% award.

Detection of the Macro test-set was down a little, mainly due to the large number of quite new viruses added for this test. Some of the early class infectors were detected, but some older polymorphic macro viruses, such as WM/Junk-Face.C and W97M/Minimorph.A, were still missed and with the increasing use of polymorphism in macro viruses this is of some concern.

*iRiSAV's* speed is acceptable, displaying throughput a tad above 1 MB/s. The single false positive identification of HLLP-1F50 should be easily fixed.

## Kaspersky Lab AVP v3.0.125 24 Oct 1998

| | | | |
|---|---|---|---|
| ItW Boot | 100.0% | Macro | 98.6% |
| ItW File | 100.0% | Polymorphic | 100.0% |
| ItW Overall | 100.0% | Standard | 100.0% |

The near-legendary detection capabilities of *AVP* did not fail it in this test, with it again performing at VB 100% award level when faced with the combined ItW Boot and File test-sets.

Normally there should be little to add to that already said of the *Data Fellows FSAV* product in commenting on *AVP*, as the same engine build level and identical virus definition (AVC) files were supplied with both products. Surprisingly, however, some macro viruses which *FSAV* detected *AVP* missed, and, contrarily, XM/Compat was reliably detected by *AVP*, thus explaining the latter's better score against the Polymorphic set. As always, *AVP* would not win any awards for its speed.

## NAI McAfee VirusScan v4.0.1.4001

| | | | |
|---|---|---|---|
| ItW Boot | 100.0% | Macro | 98.2% |
| ItW File | 100.0% | Polymorphic | 98.0% |
| ItW Overall | 100.0% | Standard | 100.0% |

This is the first hybrid *VirusScan*, combining the *Dr Solomon's* virus detection engine with *NAI's* user interface code, to be tested by *VB*. Given that both its progenitors did so a year ago, all but the most cynical would have expected it to perform at VB 100% levels on the combined ItW test-sets. It did not disappoint in this regard.

In the Polymorphic test-set, eight Marburg-infected EXEs and all but one of the W97M/Splash.A samples were missed. The very newest macro viruses and a few of the complex polymorphic ones accounted for the misses in the Macro test-set.

No false positives were recorded against the Clean test-set and the scanning speed resulted in a quite acceptable 1.7 MB/s throughput.

## Norman ThunderBYTE v8.09 27 Oct 1998

| | | | |
|---|---|---|---|
| ItW Boot | 100.0% | Macro | 93.8% |
| ItW File | 99.6% | Polymorphic | 95.4% |
| ItW Overall | 99.7% | Standard | 98.8% |

A perfect detection score on the ItW Boot tests was not matched on the ItW File tests, so *ThunderBYTE* missed a VB 100% award for the second consecutive review. The culprits were four of the Marburg EXE samples, three TMC_Level-69 COM replicants and one sample of each of the CIH variants on the WildList.

Approximately a third of the Marburg samples in the Polymorphic test-set were also missed, as were all the Compat.A and Splash.A samples and three Mad.3544 replicants. Despite detecting many of the Class variants, other polymorphic macro viruses featured among the misses on the Macro test-set. The Navrhar VxDs and a few recent additions to the Standard set were mainly responsible for the less than complete detection there.

If outright speed is as important to you as good virus detection, then *TBAV* may well be your choice. Returning a throughput close to 6 MB/s it was more than twice as fast as all but two of its rivals, although this speed is close to 25% down on that recorded by v8.04 a year earlier. No false positives were recorded.

## Norman Virus Control v4.60.19 26 Oct 1998

| | | | |
|---|---|---|---|
| ItW Boot | 100.0% | Macro | 94.0% |
| ItW File | 100.0% | Polymorphic | 99.0% |
| ItW Overall | 100.0% | Standard | 99.7% |

Another consistently good performer against the viruses on the WildList, the other *Norman* product *Norman Virus Control* (*NVC*) scoops up its sixth VB 100% award here.

As with its stablemate, *ThunderBYTE*, Navrhar was missed in the Standard and Macro test sets as was DNA.1206 in the Standard set. All the rest of *NVC's* misses were macro viruses, with it failing to detect Compat.A and Splash.A in the Polymorphic set and a slightly smaller subset of the newer and polymorphic viruses in the Macro test-set.

Scanning speed against the Clean test-set was a respectable 1.7 MB/s. Unusually for *NVC*, it reported 16 viruses in the Clean set. This should be easily fixed however, as only two 'viruses' are claimed to make up these sixteen reports –with two instances of Missilena.Trojan and the rest claimed as Zombie_II.7320 infections.

## Sophos Anti-Virus v3.15 2 Nov 1998

| | | | |
|---|---|---|---|
| ItW Boot | 100.0% | Macro | 92.2% |
| ItW File | 100.0% | Polymorphic | 100.0% |
| ItW Overall | 100.0% | Standard | 99.2% |

Also in the running for its sixth VB 100% award, *Sophos Anti-Virus* was not let down by its DOS scanner. *SWEEP* also performed well against the Polymorphics, reliably detecting all samples of the macro viruses recently added to the set.

The large influx of very new macro viruses took something of a toll on *SWEEP's* detection on the Macro test-set when compared to its performance on recent comparatives. It did, however, detect some of the viruses in the Class family and other class infectors. It also detected most of the older polymorphic viruses in the Macro test set.

Speed tests achieved a throughput of about 1 MB/s. As with other products where a direct comparison can be made, *SWEEP's* speed against the Clean test-set has dropped modestly since the previous DOS comparative – an expected result given the large growth in virus numbers and similar test conditions. No false positives were recorded.

## Symantec Norton AntiVirus v4.0 28 Oct 1998

| | | | |
|---|---|---|---|
| ItW Boot | 100.0% | Macro | 99.1% |
| ItW File | 100.0% | Polymorphic | 98.7% |
| ItW Overall | 100.0% | Standard | 99.7% |

Although sporting fewer 100% categories than some others, *Symantec's NAV* detected more samples and more viruses than any other product in this test. Importantly though, it missed none in the joint ItW test-sets, but its only miss in the Polymorphic set was a Marburg sample, and that is in the wild.

Its other misses were Win95/Boza.D in the Standard set and a smattering of very new strains amongst the macro viruses. Scanning speed was around the comfortable 1 MB/s rate and, correctly, no alarms were raised against the Clean set.

### Closing Comments

It is encouraging to see most products catching up with the demands of newer viruses. One wonders whether the results against the class infectors and other polymorphic macro viruses might have been quite different had the tests been run against products just a few weeks older.

**Technical Details**

**Test Environment:** Server: *Compaq* Prolinea 590, 80 MB of RAM, 2 GB hard disk, running *NetWare 3.12*. Workstations: Three 166 MHz Pentium-MMX workstations with 64 MB of RAM, 4 GB hard disk, CD-ROM drive and a 3.5-inch floppy, all running MS-DOS 6.22 and *Novell* ODI/VLM drivers. The workstations could be rebuilt from image backups and the test-sets were in a read-only directory on the server. All timed tests were run on one workstation that was not connected to the network for the duration of the timed tests, but otherwise configured identically to the detection test condition.

**Virus Test-sets:** Complete listings of the test-sets used are at http://www.virusbtn.com/Comparatives/DOS/199901/test_sets.html. A complete description of the results calculation protocol is at http://www.virusbtn.com/Comparatives/Win95/199801/protocol.html.

# PRODUCT REVIEW

## CA InoculateIT for NT v4.5

*Martyn Perry*

With anti-virus vendor consolidations occurring all the time, it is interesting to see an old favourite re-packaged under a new guise, along with the improvements (or otherwise) made as a result of confederation. This month we look at the reincarnation of *Inoculan* under its new *Computer Associates* (*CA*) branding of *InoculateIT*.

### Presentation and Installation

The product comes boxed with a Getting Started manual and a CD. On the CD itself are several other document files in *Acrobat* format. These include Client Agents for WinNT and InoculateIT for Windows NT. In addition, there are files covering the protection features offered for handling email on *Microsoft Exchange*, *Lotus Notes* and the Internet. Unfortunately, no licence information was provided with the review copy.

*InoculateIT for NT* requires 20 MB of hard disk for a standalone installation rising to 40 MB when distributing *InoculateIT* to other PCs. It needs 32 MB of RAM and can run on workststation and server variants of *NT* from v3.51 onwards. The product installs from CD using *Computer Associates CA-Install*. This produces the initial screen which displays the list of the Enterprise Edition products.

This is one of the few occasions when the Enterprise Edition is specifically mentioned. It can be a little confusing since the Getting Started manual introduces the product as *InoculateIT Workgroup Edition*. This list is split by platform and by product. On expansion, the platform choices offer Macintosh, *Windows 3.x*, *Windows 95*, *Windows NT(x86)*. Product options are *InoculateIT Server*, *Lotus Notes*, *Microsoft Exchange*, *Internet Protector* and *InoculateIT Client Agent*.

Choosing the *InoculateIT Server* option prompts for name and organization, then offers the choice of an Express or a Custom setup. The former automatically includes InoculateIT, AutoDownload and Alert Software. The Custom setup offers individual selection of those components plus NetWare Domain Management.

The Express setup was chosen for testing. This selects the above options, creates the program groups and icons along with configuring appropriate registry settings. There are further options to install Internet Plug-ins, Start-up options and NetWare Domain Management support. Selection of the InoculateIT and the Alert home directories follows. The Alert module provides external communication in the event of a virus incident. The final selection enables Real-time Quick Access Monitor to load at startup.

Installation then progresses with the copying of files. While this occurs, various marketing notes are displayed. Some people may find this irritating, but I feel that it serves a useful function, showing that the installation is progressing. After the anti-virus installation is completed, the user is presented with the offer to run *CA's* Unicenter TNG Framework setup Wizard. For the purposes of this article, this offer was declined.

### Security Domain Management

Domain Manager is used to include servers in *InoculateIT* domains and to configure on-access protection for these servers. Each *InoculateIT* domain requires a master server, which sends management information to all other servers within the domain. Any server can be selected as the master and other servers can be added to the domain as required.

*InoculateIT* servers send periodic broadcasts allowing the master server to recognise them. In some networks, this broadcast information may be filtered, thereby preventing recognition. To cater for this, there is a point-to-point management option to allow communication. Machines located in this way cannot be included as part of an *InoculateIT* domain and will need separate administration. Having grouped the servers into a domain, they can be given virus protection by configuring real-time support.

### Real-time Scanner

Real-time scanning can be set to check incoming files only, outgoing files only, both or be disabled. The default file extensions to scan are COM, DLL, DOC, DOT, EXE, RTF, SYS, VXD and WIZ. There is also a facility to check 'compressed' files, with the default extensions being ARJ, LHA, LZH, MIM, UUE and ZIP.

Both those lists are user-modifiable. Another option is Exclude Specified Files. The default list in this instance is BTR, DB, DBF, MDB, MDX, NDX, SBF. This list is provided to help performance on large data files, but having MDB as a default option may lead to vulnerability, as we will see in the virus test, and this list will need to be reassessed on a regular basis as macro viruses are developed for more platforms.

In the event of a virus being detected, a selection of action options are available. Report Only means that no action is taken and just a result is displayed. Delete File is self-explanatory and Rename File changes the file extension to AVB. Cure File is an option applicable to macro viruses, providing the facility to remove viral, or all, macros.

Further options include copying the file before curing where the default destination is C:\Inoculan\VIRUS, or renaming the file if a cure fails (default AVB). Move File

repositions a file to default destination C:\Inoculan\VIRUS, while Purge File deletes it with no recovery. The effect of choosing the Rename and Move File option should be guessed easily. For scan types there is the choice of Fast scan, Secure scan (default) and Reviewer scan. With each, there is the opportunity to include heuristic scanning.

'Protected areas' defines which devices can be protected. These include floppy drives, CD-ROM drives and email, provided that the appropriate email protection facility has been installed. For network drives, *InoculateIT* will scan files moving between mapped drives, even if no file passes the hard drive of the local machine.

Advanced Protection facilities include Virus-wall Incoming mode which prevents infected files from being copied to the server and overwriting clean versions. Currently, this is limited to EXE, COM, DOC, DOT and XLS files. The 'allow fast backup' option ensures that files can be copied to tape, during a backup session, without being scanned. *InoculateIT* will skip files being opened by backup software to improve performance. There is a Report User Name which allows *InoculateIT* to report the name of the user trying to pass the virus.

Finally, the Quarantine option can block user access to the server for a configurable time. The quarantined users can be located in the Quarantine tab under the Real-time Monitor options screen, and the administrator can release users from quarantine by removing their names from this list. The quarantine period is applied to users with administrator rights but not to the Administrator account itself.

### Scheduled Scan

Together with the scheduled scan configuration there is a Targets/Schedule tab. This gives the choice of target drives to be scanned in addition to making refinements to the selected directories by simply clicking the required location. I find this visual approach to target selection very easy to work with and allows immediate confirmation of selections made. In addition, specific files and/or directories can be excluded by adding to an exclusion list.

To help manage server performance, the CPU load of scheduled scans can be limited. The schedule for the scan may be initiated at start up or at a defined date and time. Scheduled scans can be repeated using a combination of settings for Months, Days, Hours and Minutes. Each can be defined independently giving a very flexible set of choices. The file types to be included in the scan are the same as local scan (see below) with the addition of XLA. Moreover, there is an option to scan migrated files. The files to be excluded are also the same as for local scan.

### Manual/On Demand Scan

The Local scanner option is for workstation scanning and specific mapped drives on servers. Local Scanner Options allow for the scanning of All Files, Executable files or has an option to Exclude Specified Files. For the Executable files, the default file extensions are COM, DLL, DOC, DOT, EXE, RTF, SYS, VXD, WIZ, XLS, XLT and XLW.

There is a separate selection for 'compressed' files where the extensions are ARJ, LHA, LZH, MIM, UUE and ZIP. The Exclude File list has a default set of BTR, DB, DBF, MDB, MDX, NDX and SBF. As mentioned earlier, this list needs careful selection to avoid compromising security for the sake of performance – often a delicate balancing act.

### Administration and Updates

The main menu options are Domain Manager, Local Scanner and Service Manager. The latter deals with the support services for *InoculateIT*, including Automatic Startup, while the Manual option gives the user control as to when the service start.

Other options include how long to keep scheduled jobs in the queue when finished and provide an Active Server timeout to determine how long to wait before setting a server in the domain as inactive. There is an Event Log which can be configured to the number of messages to be stored and how long to keep them before purging from the list. To help limit the size of the log, a filter can be used to choose the level of severity of the messages to keep – Critical, Warning, or just Informational.

A separate service allows the virus directory to be purged either immediately on selection or after a defined number of days. Another provides for the configuration of network broadcasts. These can use the mailslot protocol (for *NT* domains) or SMTP (for TCP/IP networks) in combination or individually. Although there are no specific hardcopy reports, the status of scan progression and summary results are always available for display. Hardcopy is handled by printing trouble tickets via Alert Service.

The Alert module allows detection alerts to be sent to different users via various methods of communication including network broadcast, pager, email, hardcopy, SNMP, *NT* event log, and *CA-Unicenter TNG*. The Alert option was not activated for the purpose of the testing. The Virus Pattern File used for testing was v4.12 20/8/98. Updates are available from *CA* by FTP or modem.

### Detection Rates

The scanner was checked using the standard *Virus Bulletin* test-sets – ItW Boot and File, Standard, Polymorphic, and Macro. Full test details are included in the summary. The tests were conducted using the default scanner file extensions supplied. The scan action option was selected to delete the infected files. The residual file count was then used to determine the detection rate.

Against the Standard and Boot Sector test-sets *InoculateIT* gained 100% detection rate. However, it failed to detect 21 samples from the ItW test-set, and missed 52 samples in

the Macro set. These last included all eight samples in the *Access 97* set, which was due to the default settings excluding MDB files. When the MDB extension was removed from the exclusion list, all eight samples were then detected. Also, when the SCR extension was added to the executables list, three further samples of TPVO.3783.A were detected.

The rest of the undetected samples consisted of eighteen samples of Marburg – the main culprit in the poor showing against the Polymorphic test-set where all 744 Marburg samples were missed. The only other Polymorphic problem was missing eleven samples of Cryptor.2582.A.

### Speed and Real-time Scanning Overhead

To determine the on-access scanner's impact on the server, the following test was timed. 200 files of 21.24 MB (EXE and COM) were copied from one folder to another using XCOPY. The folders used for the source and target were excluded from the virus scan so as to avoid a file being scanned while waiting to be copied.

The default setting of Maximum Boost for Foreground Application was used in all cases. Due to the different processes which occur within the server, the tests were run ten times for each setting and an average taken. The tests were as follows:

- Program not loaded: establishes the baseline time for copying the files on the server.
- Program installed but not scanning, Real-time disabled: tests the impact of the application in a quiescent state.
- Program loaded, Real-time enabled, Incoming Files only: tests the impact of the scan on incoming files.
- Program loaded, Real-time enabled, Outgoing files only: tests the impact of the scan on outgoing files.
- Program loaded, Real-time enabled, Incoming and Outgoing Files: tests the impact of the scan for incoming and outgoing files.
- Program loaded with Real-time enabled, Incoming and Outgoing Files; Manual scan also included: tests the full impact of scan for incoming and outgoing files as well as the normal scanning of files.
- Program unloaded: run after the other tests to check how well the server is returned to its former state.

Two sets of timing tests were run, one with Secure Scan selected, the second with Fast scan. The difference in times was about 5% which suggests that the default selection of Secure Scan is suitable for most situations. The results reported below are from the Secure Scan tests.

The one notably odd result came after uninstalling the software, when the timing jumped significantly. This test was run without downing the server and flushing the memory and so can probably be ascribed to a 'dirty' environment. However, it highlights the need to clean up fully after uninstalling software.

### Summary

The documentors seem to be ahead of the developers. They call the home directory InoculateIT when the server version still uses Inoculan, but the *Windows 95* client version has been updated. It may be a small point, but attention to such details, and consistency, are marks of quality control. Although there is no virus encyclopaedia or virus listing with descriptions, there is still generic support in the documentation for dealing with virus incidents.

The issue of inclusion/exclusion in a scan selection of specific files or file types is always open to debate. On the one hand there is always performance to consider, but this has to be weighed against security – perhaps MDB files should be covered during a scheduled scan but not a real-time one. Therefore it remains a case of 'caveat emptor' – watch out when buying a cave. Apart from tidying up the detection, overall, the transition of the product seems to have been achieved successfully.

## CA InoculateIT for NT Server v4.5

Detection Results

| Test-set[1] | Viruses Detected | Score |
|---|---|---|
| In the Wild Boot | 84/84 | 100.0% |
| In the Wild File | 718/739 | 97.2% |
| Standard | 1026/1026 | 100.0% |
| Polymorphic | 13689/14444 | 94.8% |
| Macro | 1723/1723 | 100.0% |

Overhead of On-access Scanning:

The tests show the time (in seconds) taken to copy 200 COM and EXE files (21.2MB). Each test was repeated ten times, and an average taken.

| | Time | Overhead |
|---|---|---|
| Not loaded | 17.4 | – |
| Loaded, disabled | 20.9 | 19.5% |
| — + incoming, no scanning | 34.7 | 98.2% |
| — + outgoing, no scanning | 32.8 | 87.5% |
| — + both, no scanning | 33.7 | 92.9% |
| — + — + on-demand scan | 91.9 | 425.8% |
| Program unloaded | 105.1 | 500.9% |

**Technical Details**

**Product:** *CA InoculateIT for NT Server v4.5.*

**Developer/Vendor:** *Computer Associates Inc*, 1 Computer Associates Plaza, Islandia, NY 11788, USA. Tel +1 516 3426000, fax +1 516 3425118, email info@cai.com., and WWW http://www.cai.com/.

**Price:** $695 single-server licence. Client licences are separate and start at $49 each.

**Test Environment:** Server: *Compaq* Prolinea 590, 80 MB of RAM, 2 GB hard disk, running *NT Server v4.0 (SP3).*

[1]**Virus Test-sets:** Complete listings of the test-sets used are at http://www.virusbtn.com/Comparatives/DOS/199901/test_sets.html.

**SUBSCRIPTION RATES**

**Subscription price for 1 year (12 issues) including first-class/airmail delivery:**

UK £195, Europe £225, International £245 (US$395)

**Editorial enquiries, subscription enquiries, orders and payments:**

*Virus Bulletin Ltd*, The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP, England

Tel 01235 555139, International Tel +44 1235 555139
Fax 01235 531889, International Fax +44 1235 531889
Email: editorial@virusbtn.com
World Wide Web: http://www.virusbtn.com/

**US subscriptions only:**

*Virus Bulletin*, 18 Commerce Way, Woburn, MA 01801, USA

Tel (781) 9377768, Fax (781) 9320251



# END NOTES AND NEWS

***Sophos* will be hosting an introductory computer virus workshop on 10 March 1999 to be followed on 11 March by an advanced session.** The two-day course will be held at the organization's training suite in Abingdon, UK. To register for a place, contact Karen Richardson; Tel +44 1235 544015, fax +44 1235 559935, or find details at http://www.sophos.com/.

The *Microsoft Security Partners Program* now includes three *Data Fellows* products – *F-Secure Workstation Suite*, *F-Secure VPN+* and *F-Secure FileCrypto*. In an unrelated announcement ***Data Fellows* has formed an alliance with *Sonera***, a leading Finnish telecommunications company to provide Intranet and extranet services. *Data Fellows' F-Secure* technology is to be used in the creation of a secure IP service platform. For further information contact Jukka Kotovirta; Tel +358 9859900, fax +358 985990599, or visit the *Data Fellows* web site http://www.DataFellows.com/.

***Central Command*, the US distributors of *AVP*, is running bi-monthly advanced computer virus workshops** aimed at System Administrators. The classes will be held at the company's corporate headquarters in Brunswick, Ohio. Class size is limited to 25, and the cost for the three-day workshop is $1695. Contact Renée Barnhardt; Tel +1 330 273 2820 or email renee@avp.com.

***Trend Micro's InterScan VirusWall* has been tested and approved by *Sun*** for use scanning inbound and outbound SMTP traffic on *Sun Internet Mail Server* software. It is available now for £1295 for 50 users. For details contact Steve White at *Peapod, Trend's* UK distributors; Tel +44 181 6069924 or email trend@peapod.co.uk.

***CSI Educational Resource Center* is adding extra classes to its 1999 programme of seminars** ranging from 'An Introduction to Computer Security' to 'Advanced Windows NT Security'. The seminars are held in major cities across the United States. ***CSI*'s 9th Annual Network Security Conference,** *NetSec'99*, is to be held from 14–16 June, 1999, in St Louis, Missouri at the Hyatt Regency Hotel. Over 1500 computer and information security professionals are expected to attend the conference and its concurrent exhibition. For a new calendar of events or more details on the conference, contact *CSI*; Tel +1 415 9052626, fax +1 415 9052218, email csi@mfi.com or visit the CSI web site at http://www.gocsi.com/.

***Network Associates Inc* is to host a two-day live virus workshop from 23–24 February 1999.** The sessions are to take place at the *NAI* Training Centre in Aylesbury, UK from 9.30am to 4.30pm. For more information contact Caroline Jordan; Tel +44 1296 318881 or email caroline_jordan@nai.com.

***eicar's* 1999 conference 'E-Commerce and New Media: Managing Saftey, Security and Malware Challenges Effectively' is to be held in Aalborg, Denmark from 28 February–2 March.** On Saturday 27 *eicar* committee meetings are scheduled. Two workshops take place on Sunday 28 February – 'Encryption and Privacy: The Global Policy Disorder' in the morning, followed by 'Managing Privacy and Security Software, Systems Management and Policy Issues' in the afternoon. *eicar* working groups are to meet from 17.00–18.30 that day. Delegates are reminded that they must pre-register with *eicar* for all the meetings and workshops. The conference itself will be opened by Rainer Fahs, chair of *eicar*, on Monday 1 March – speakers include Sarah Gordon, David Harley and Marko Helenius. An exhibition will run for three days starting on Sunday 28 February at 10.30am. Contact Professor Urs E Gattiker of Aalborg University; Tel +45 96358962, fax +45 98153030 or email Urs_the_Bear@bigfoot.com, or visit http://www.eicar.dk/, for more information.

**Registrations are now being taken for *the Internet Society's* 1999 Network and Distributed System Security (NDSS) Symposium.** The 6th annual NDSS Symposium provides a mix of technical papers and panel presentations, covering all aspects of Internet security. Associated features include pre-conference technical tutorials and sponsorship opportunities. It takes place from 3–5 February 1999 at the Catamaran Resort Hotel in San Diego, California, USA. For more information contact the Internet Society; 12020 Sunrise Valley Drive, Reston, VA 20191, USA, tel +1 703 648 9888, fax +1 703 648 9887, or email ndss99reg@isoc.org. On-line information is available at http://www.isoc.org/ndss99/.

**WebSec'99 is to be held at the Mount Royal Hotel in London, UK from 23–25 March 1999.** Optional pre- and post-conference workshops will run on 22 and 26 March. For more information on the conference or the concurrent exhibition contact the organizers; tel +44 171 7798944, fax +44 171 7798293, email misuk@misti.com or visit http://www.misti.com/.